REMARKS

Claims 1-7 are pending in the above-identified application. Claims 1 and 4-7 were rejected. Claims 2-3 were objected to as being dependent upon a rejected base claim but deemed allowable if rewritten in independent form to include the limitations of the base claim and any intervening claims. Applicants thank the Examiner for acknowledging the patentable subject matter of these claims. With this Amendment, claims 1, 6, and 7 were amended to correct for cosmetic and grammar informalities. Claim 2 was written in accordance with the Examiner's suggestions to place this claim and its dependent claim 3 in condition for allowance. Accordingly, claims 1 and 4-7 remain at issue.

I. 35 U.S.C. § 102 Anticipation Rejection of Claims

Claims 1 and 4-7 were rejected under 35 U.S.C. § 102(e) as being anticipated by *Chen et al.* (Patent 6,687,725). Applicant respectfully traverses this rejection.

With respect to independent claim 1, Applicant claims a circuit design method executed by a computer for designing a processing circuit for processing on a finite field in which the method includes the following limitations, among others:

> *a first step of obtaining a first primitive root α_1 on the basis of a first polynomial for a first extension from a first finite field to a second finite field, the first polynomial having a 0-th term;*
>
> *a second step of obtaining a second primitive root α_2 on the basis of a second polynomial for a second extension from said second finite field to a third finite field, in which a coefficient of the 0-th term of the second polynomial is defined using said first primitive root α_1 and the coefficient of the 0-th term of said first polynomial...*

Independent claims 6 and 7 have limitations similar to these claim 1 limitations.

Applicant teaches that by utilizing the method of claim 1 a processing circuit for processing on a finite field is formed with a decreased number of circuit elements in comparison to conventional processing circuits formed for processing on a finite field. See Application, at pg. 20, line 17- pg. 21, line 9.

Chen discloses an arithmetic circuit for performing basic operations in a finite field, $GF(2^m)$, such as a multiplication (A*B) operation, exponential operation B^N, and inverse multiplication operation (B^{-1}). *Chen* further discloses the arithmetic circuit has a calculating processor (CP) that is configured to calculate (A*B) and ($A*B^2$) based on a first primitive polynomial F(x) of the finite field $GF(2^m)$ where the first primitive polynomial F(x) has a first primitive root (α) and a 0-th term of f_0. *See Chen*, Col. 4:50-Col. 5:25. However, *Chen* fails to disclose forming an embodiment of the calculating processor (CP) or any other component of the disclosed arithmetic circuit by "*obtaining a second primitive root α_2 on the basis of a second polynomial for a second extension from [the] second finite field to a third finite field, in which a coefficient of the 0-th term of the second polynomial is defined using said first primitive root α_1 and the coefficient of the 0-th term of said first polynomial*" as taught and claimed by Applicant.

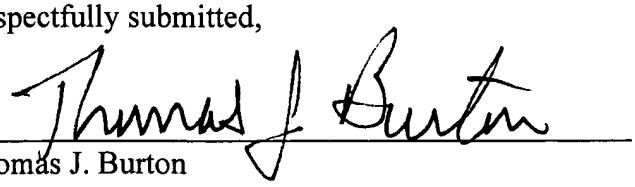
Thus, Applicant submits that *Chen* fails to teach all the limitations of claims 1, 6, or 7. Accordingly, Applicant respectfully requests that the rejection to claims 1, 6, and 7 be withdrawn.

Claims 4 and 5 depend from claim 1 and should be deemed allowable for at least the same reasons as claim 1.

II. Conclusion

In view of the above amendments and remarks, Applicant submits that all claims are clearly allowable over the cited prior art, and respectfully requests early and favorable notification to that effect.

Respectfully submitted,

Dated: December 2, 2005 By: 

Thomas J. Burton
Registration No. 47,464
SONNENSCHEIN NATH & ROSENTHAL LLP
P.O. Box 061080
Wacker Drive Station, Sears Tower
Chicago, Illinois 60606-1080
(312) 876-8000